(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10123950 A**

(43) Date of publication of application: **15 . 05 . 98**

(51) Int. Cl **G09C 1/00**

(21) Application number: **08278423**

(22) Date of filing: **21 . 10 . 96**

(71) Applicant: **FUJI XEROX CO LTD**

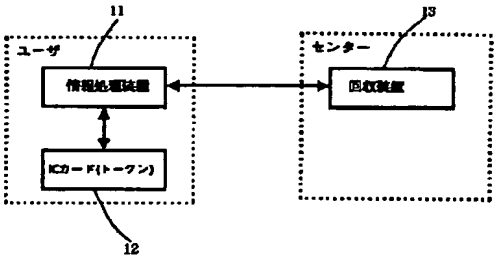
(72) Inventor: **SAITO KAZUO**
SHIN YOSHIHIRO
TAKEDA YUKIFUMI

(54) DATA VERIFICATION METHOD, VERIFIED DATA GENERATION DEVICE, AND DATA VERIFICATION DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To make it possible to use a protection device with a low calculation ability and a small storage capacity when securing to safely transmit or keep data like a history of utilization by adding verification value to them.

SOLUTION: A token 12 generates information on the utilization history and sends it to an information processing device 11, and also generates a verification value for holding it to a verification value holding part 21. The information processing device 11 records the information on the utilization history in a history holding part 16. The token 12 provides the verification value with a signature when requested for a verification output from the information processing device. The information processing device 11 outputs the information on utilization history and the verification value with the signature to a recovery device 13. The recovery device 13 verifies the signature, and further, verifies the history of utilization based on the verification value.



Requested document: JP10123950 click here to view the pdf document

Method and apparatus for data verification

Patent Number: EP0837383
Publication date: 1998-04-22
Inventor(s): SAITO KAZUO (JP); TAKEDA KOJI (JP); SHIN KILHO (JP)
Applicant(s):: FUJI XEROX CO LTD (JP)
Requested Patent: JP10123950
Application Number: EP19970118074 19971017
Priority Number(s): JP19960278423 19961021
IPC Classification: G06F1/00
EC Classification: G06F1/00N7R2, G06F1/00N7A, H04L9/32B
Equivalents: US6161183

Abstract

A token 12 creates utilization history information and sends the information to an information processing unit 11 and simultaneously creates an verification value and stores the value in a utilization-value holding unit 21. The information processing unit 11 records the utilization history information in a history holding unit 16. On receiving a verification-value output request from the information processing unit 11, the token 12 provides the verification value with a signature and outputs the combination of the verification value and the signature. The information processing unit sends to a recovery unit 13 the verification value with the signature as well as the utilization history information. The recovery unit 13 verifies the signature and also the utilization history on the basis of the verification value further.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平10－123950
(43)公開日　平成10年(1998)５月15日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ

審査請求　未請求　請求項の数21　ＯＬ　（全 28 頁）

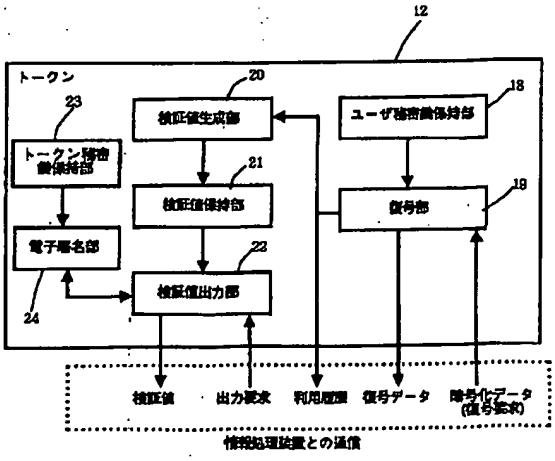
(21)出願番号　特願平8－278423

(22)出願日　平成８年(1996)10月21日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　齊藤　和雄
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　申　吉浩
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　竹田　幸史
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　データ検証方法、被検証データ生成装置およびデータ検証装置

(57)【要約】
【課題】　利用履歴のようなデータに検証値を付加して安全に伝送あるいは保持を確保する際に、計算能力が低く、記憶容量も小さい防御装置を用いることができるようにする。
【解決手段】　トークン１２は利用履歴情報を作成して情報処理装置１１に送るとともに検証値を生成し検証値保持部２１に保持する。情報処理装置１１は利用履歴情報を履歴保持部１６に記録する。トークン１２は情報処理装置１１から検証値出力が要求されると検証値に署名を施して出力する。情報処理装置１１は利用履歴情報および署名付き検証値を回収装置１３に送出する。回収装置１３は署名を検証し、さらに検証値に基づいて利用履歴の検証を行う。



【特許請求の範囲】
【請求項1】　順次に生成される複数のデータ本体の各々について、当該データ本体と、当該データ本体に先行するデータ本体の検証値とから当該データ本体の検証値を、防御された装置の内部において、生成するステップと、
一度に検証される複数のデータ本体の内の最後のデータ本体に対して生成された検証値に上記防御された装置の内部においてデジタル署名を施して署名付き検証値を生成するステップと、
上記署名付き検証値を、上記防御された装置の外部に送出するステップと、
上記複数のデータ本体と上記署名付き検証値とに基づいて上記複数のデータ本体を検証するステップとを有することを特徴とするデータ検証方法。
【請求項2】　順次にデータ本体を生成する手段と、
検証値を保持する検証値保持手段と、
上記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とから新たな検証値を生成し、上記新たな検証値で上記検証値保持手段に保持されている検証値を更新するする検証値生成手段と、
所定のタイミングにおいて上記検証値保持手段に保持されている検証値に署名を施す署名手段とを有し、
さらに上記検証値生成手段、検証値保持手段および上記署名手段を防御された装置内に設けることを特徴とする被検証データ生成装置。
【請求項3】　順次に生成された複数のデータ本体と、上記複数のデータ本体から計算された検証値に署名が施された署名付き検証値とを受け取る手段と、受け取った上記署名付き検証値の署名を検証する署名検証手段と、上記署名検証手段により署名の検証された検証値から、受け取った上記複数のデータ本体が正しいことを検証する検証手段とを有することを特徴とするデータ検証装置。
【請求項4】　複数の連続した履歴データからなる履歴データ群に対して、順次計算される唯一の検証値のみを防御された装置内に保持し、上記検証値を上記防御された装置の外部に出力する際には、上記検証値のみにデジタル署名を施すことを特徴とする履歴保持方法。
【請求項5】　複数の連続したデータを入力するためのデータ入力手段と、
上記データを処理するためのデータ処理手段と、
上記データの処理に関連する履歴データと、その時点で保持する検証値を入力として、検証値を生成するための検証値生成手段と、
生成された上記検証値を保持するための検証値保持手段と、
該検証値に対して署名を施すための署名手段とを有し、少なくとも上記検証値生成手段、上記検証値保持手段および上記署名手段を防御された装置内に保持することを特徴とした履歴保持装置。
【請求項6】　上記検証値生成手段に用いる計算が一方向性関数である請求項5記載の履歴保持装置。
【請求項7】　上記履歴データの形式が、履歴データ本体とその履歴データを処理した時の検証値との組である請求項5または6記載の履歴保持装置。
【請求項8】　データを処理する毎にカウントするカウンタ手段を有し、上記履歴データ群における履歴データの形式が、データを処理した時のカウンタの値と履歴本体からなる請求項5、6または7記載の履歴保持装置。
【請求項9】　利用者の出力要求に応じて、署名された検証値を出力する請求項5、6、7または8記載の履歴保持装置。
【請求項10】　上記履歴保持装置が単一のＣＰＵとソフトウェアで構成され、データ処理手段によるＣＰＵの負荷が低い時に上記署名手段が、適宜検証値に署名した検証値を作成して出力する請求項5、6、7、8または9記載の履歴保持装置。
【請求項11】　データ処理手段と、
上記検証値を出力した時点で上記データ処理手段の機能を停止し、外部から正当な命令が与えられまではそデータ処理手段の機能を停止する機能停止手段とをさらに有する請求項5、6、7、8、9または10記載の履歴保持装置。
【請求項12】　機能を停止させるための停止条件保持手段を有し、停止条件保持手段に記述されている条件を満たした時には、上記機能停止手段が上記検証値に署名した署名付き検証値を出力して、機能を停止する請求項11記載の記載の履歴保持装置。
【請求項13】　外部の正当者の公開鍵を保持するための正当公開鍵保持手段を有し、上記機能停止手段が、機能を復帰させるために受け付ける命令が、最後に出力した検証値に外部の正当者が電子署名を施したものであって、上記機能停止手段が命令を受け取った時に該正当公開鍵保持手段に保持されている公開鍵で署名を検証し、さらに署名されている検証値が、上記検証値保持手段に保持されている検証値と等しいかどうかを確認する請求項11または12記載の履歴保持装置。
【請求項14】　複数の連続する履歴データ群とそれらのデータ群から計算された検証値に署名が施された署名付き検証値を入力するためのデータ入力手段と、
入力した上記署名付き検証値の署名を検証するための署名検証手段と、
入力した上記データ群と署名の検証された検証値とから、入力した上記データ群が正しいことを検証するための検証手段とを有することを特徴とする履歴検証装置。
【請求項15】　前回に入力した検証値を記憶するための前検証値記憶手段を有し、検証手段が検証する際に、該前検証値も用いる請求項14記載の履歴検証装置。
【請求項16】　上記検証手段に用いる計算が一方向性

関数である請求項１４または１５記載の履歴検証装置。
【請求項１７】　上記履歴データの形式が、履歴データ本体とその履歴データを処理した時の検証値との組である請求項１４、１５または１６記載の履歴検証装置。
【請求項１８】　上記履歴データ群における履歴データの形式が、データを処理した時のカウンタの値と履歴本体とからなる請求項１４、１５、１６または１７記載の履歴検証装置。
【請求項１９】　データを保持するためのデータ記憶手段と、
機能を停止する際のある一定の条件を保持するための停止条件保持手段と、
該停止条件保持手段に保持された条件を満たした時に機能を停止し、外部から正当な命令が与えられるまでは機能を停止しつづけるための機能停止手段と、
秘密鍵を保持するための秘密鍵保持手段と、
データ保持手段に保持されたデータ群に該秘密鍵保持手段に保持された秘密鍵を用いて電子署名を施すための電子署名手段と、
署名した電子署名を保持するための電子署名保持手段と、
外部の正当者の公開鍵を保持するための正当公開鍵保持手段とを有し、
上記機能停止手段が機能を復帰させるために受け付ける命令が、上記電子署名保持手段に保持された電子署名に対して外部の正当者が電子署名を施したものであって、機能停止手段が命令を受け取った時に該正当公開鍵保持手段に保持されている公開鍵で署名を検証し、さらに署名されている値が、電子署名保持手段に保持されている値と等しいかどうかを確認することを特徴とする履歴保持装置。
【請求項２０】　所定の条件が満たされたときに電子機器本体の少なくとも一部の機能を停止する機能停止手段と、
所定のデータを外部に出力する手段と、
上記所定のデータに署名を施して生成された署名付きデータを受信する手段と、
上記署名付きデータについて署名を検証する署名検証手段と、
上記署名検証手段によって上記署名付きデータの署名の正当性が検証されたときに上記一部の機能の停止を解除する手段とを有することを特徴とする電子機器。
【請求項２１】　順次にデータを生成する手段と、上記データ本体に対する検証値を保持する検証値保持手段と、上記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とから新たな検証値を生成し、上記新たな検証値で上記検証値保持手段に保持されている検証値を更新するする検証値生成手段と、所定のタイミングにおいて上記検証値保持手段に保持されている検証値に署名を施す署名手段とを有してなるデータ生成装置と、上記データ生成装置から出力されるデータ本体を回収するデータ回収装置との間のインターラクションを実行するためのコンピュータプログラム製品において、
上記データ生成装置から出力されたデータ本体および署名が施された検証値を記憶するステップと、
記憶された上記データ本体および上記署名が施された検証値を、所定のタイミングで上記データ回収装置に送信するステップとをコンピュータに実行させるために用いることを特徴とするコンピュータプログラム製品。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】この発明はデータを検証する技術に関し、とくに連続する大量のデータ群、例えば利用履歴のようなデータを安全に伝送あるいは保持しなければならないような情報処理装置一般に用いるのに適したデータ検証技術に関する。
【０００２】
【従来の技術】昨今のデジタル情報処理技術の発達や、情報ハイウェイ構想などにより、あらゆる情報がデジタル化され、ネットワークを通じて配付・流通される時代が到来しようとしている。すでにインターネットやパソコン通信、あるいはＣＤ－ＲＯＭという形態で、文字情報はもとより、画像、動画、音声、プログラムなどの様々な情報が配付・流通しはじめている。
【０００３】しかしながら、そのような文字、画像、動画、音声、プログラムなどの様々なデジタル情報は物理的な物とは異なって実体を持たないため、利用しなければ価値がない、複写が容易で、かつ低コストで可能である、などの特徴を持つ。しかし、現在はその所有に対して対価を支払っているため、一旦、ある人に所有された情報が複写されるということを制限している。本来、デジタル情報の最も優れた特徴であるはずの複写容易性やそのコストの低さを無理やりに封じ込めていることになる。
【０００４】これを解決するために、最近ではプログラムを代表とするデジタル情報を暗号化して自由に流通させ、利用する際には代金を支払って、デジタル情報を利用するための復号鍵を受取り、情報を復号化して利用するようなシステムも登場してきている。あるいは、情報は利用しなければ価値がないという観点から、特公平６－９５３０２号公報におけるソフトウェアサービスシステムや、特開平７－２１２７６号公報の情報利用量測定装置のような、情報の利用に対して課金するような技術が提案されている。
【０００５】これらの技術によって、パーソナルコンピュータやワークステーションなどの情報処理装置上では、ユーザはプログラムを代表とするソフトウェアを利用する際にはソフトウェアを購入して利用するのではなく、無料または非常に安価に入手し、利用した時に利用

に応じて利用料金という形で、例えば一回利用したから幾ら、というように課金がなされるようになった。

【0006】情報の利用に対して課金を行うためには、その利用の頻度に応じて個々の利用者から利用料金を回収しなければならない。あるいは場合によっては、一括回収した利用料金を情報を提供した側にその利用頻度に応じて分配しなければならない。そのためには、利用者の環境における利用の履歴を安全に記録し、そして安全に回収する必要がある。

【0007】しかし、特開平7－21276号公報では利用履歴を記録する機能として、利用量メーターは存在するが、実際にそこに記録された利用量をどのように回収するかについては触れられていない。

【0008】そのための方法としては、利用履歴を利用者が利用する情報処理装置の管理する記憶装置、例えばハードディスク装置などではなく、それとは独立した安全な装置に記録する方法がある。例えば、特公平6－95302号公報ではICカード内に利用の履歴を書き込むようにしている。

【0009】また、特開平3－25605号公報の課金情報送出方式や特開平6－180762号公報の課金情報収集システムではネットワークを通じて課金情報を回収するようにしている。

【0010】

【発明が解決しようとする課題】ICカードのような安全な装置に書き込まれた履歴を回収するためには、ネットワークで回収するか、もしくは、その装置から直接に正当な権限を持った回収者が直接的に回収する方法がある。

【0011】しかしながら、ネットワークを通じて履歴を回収する方式では、課金情報の安全性すなわち、課金情報が途中で改竄されたり、あるいは利用者が不正な課金情報を作成してそれを送ったりという安全性の面についてはまったく考慮されていなかった。従って、企業内のような一定の信頼のおけるネットワーク内においては適用可能であったが、不特定多数の個人が参加するようなインターネットには、安全性の面から適用できないという問題があった。

【0012】従って、安全にICカードのような装置内の履歴を回収するためには、その装置から直接に正当な権限を持った回収者が直接的に回収するしか方法がなかったのである。

【0013】しかし、最近になり研究の進んでいる暗号技術、特に電子署名技術を用いると、上記の問題を解決することが可能である。すなわち、安全装置に固有の秘密鍵を封入し、安全装置からデータを取り出す際には必ず署名を施す様にすればよい。これによって、データが正しいことが、データに付随している電子署名を確認することで、後から確認できるようになる。

【0014】電子署名はRSA（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号を用いる手法が広く知られている。しかし、RSA暗号による署名、あるいは、他の電子署名には、一般に非常に多くの計算量を必要とし、一回の処理に多大な時間がかかるのが普通である。従って、連続する多量のデータに対して署名を施さなければならない場合や、あるいは署名の処理を計算能力が低い計算機上で処理する場合には、非常に大きな問題となる。

【0015】利用履歴を記録するような安全装置としてICカードのような装置を用いる場合に、一般にそのようなICカードに搭載可能なCPUの計算能力は低いことが多く、多量の計算をさせると非常に時間がかかるという問題があった。あるいは、計算時間を速くするために、計算能力を高くしようとすると非常に高いコストを要するという課題があった。

【0016】また、利用の履歴データは一般に長大になるため、ICカードのような小さな装置にすべての履歴データを記録しようとすると記録容量が問題になるという課題もあった。

【0017】なお、元々RSA暗号を始めとする現代の暗号技術の安全性は計算量に基礎を置いており、計算機の能力が伸びるとそれに伴って署名や暗号に用いられる鍵長が大きくされるようになっている。従って、将来的に計算機の能力が上がれば解決するという問題ではなく、その時代における最大の処理能力を持つ計算機に比べて低い処理能力の計算機しか使えないような機器（例えば、個人が用いるトークンなど）を用いる場合には将来に渡っても常にこの問題は本質的な課題となる。

【0018】この発明はこのような事情に鑑みてなされたものであり、その目的とするところは、計算能力の低い装置に置いても、高速にデータを検証可能なデータを生成できる方法を提供することにある。

【0019】すなわち、利用履歴全体をICカード内に保持するのではなく、利用履歴から得られる検証値のみをICカード内に保持し、利用履歴の本体はユーザの管理する情報処理装置（パソコンなど）側に保持させようとするものである。

【0020】検証値の観点から従来の技術を参照すると、データ通信に使用される技術であるDES－MACと呼ばれる技術がある。MACとはＭｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅの略であり、メッセージが完全である（改竄されていない）ことを示す一定の長さを持ったコードである。オリジナルのメッセージに添付されて用いられたりする。データ通信は途中でエラーが発生することは致命的であるので、途中でデータが変わってしまったことを検知できるような構成になっている。

【0021】ここで、DESとはＤａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄの略で64ビットを一つのブロックとするブロック暗号のアルゴリズムである

（Applied Cryptography pp265）。CBC（CypherBlock Chain）モード（Applied Cryptography pp193，JIS－X5051）とはDESを代表とするブロック暗号の使い方の一種であり、個々のブロックを独立させて暗号化していくのではなく、直前の暗号化されたブロックとこれから暗号化しようとするブロックの排他的論理和を取り、それをDESの入力とする方式である。この方法だと同じ内容のブロックを暗号化した時にでも、それまでに暗号化したブロックが異なれば暗号化した結果も異なることになる。

【0022】DES－MAC（CBC－MACについてApplied Cryptography pp455を参照）は、DESにおけるCBCモードを応用したものであり、最後に得られたブロックをデータストリーム全体の検証値に用いようとするものである。

【0023】DES－MACの構成を図21に示す。図の上部が伝送しようとするデータストリームであり、データストリームはそれぞれ64ビットづつのブロックに分割される。IVとはInitial Vectorの略で乱数で生成された初期値である。分割されたブロックはDES－CBCモードと同様に連鎖的にDES暗号器を通していき、先頭にIVを、そして最後に得られたブロックを伝送しようとするデータストリームの検証値を付加して伝送される。受信した側ではこの処理と逆の処理を行って得られた検証値が、等しくなるかどうかを検証する。

【0024】しかし、このような処理方法は基本的に通信によってデータを伝送することを目的としているものであり、送信者は完全なデータを短時間、確実に保持することが前提となっていることから、完全な履歴の回収に適用しようとすると、問題を生じる。すなわち、履歴データは長期に渡って蓄積され、その間ユーザの恣意的な管理や、システムの事故などの危険に曝される可能性があるからである。

【0025】第一に上記の方法（DES－MAC）ではデータブロックが連続して伝送されることを前提としている。すなわち、通常データの伝送にはさらに下位の層が存在し（TCP／IP：トランスミッション・コントロール・プロトコル／インターネット・プロトコルではTCP層が相当する）、その層によってデータブロックの順番が保証されることになる。

【0026】しかしながら、利用履歴の場合には、ユーザの管理下に置いてしまうと、その時点で履歴の順序は保証されなくなってしまう。すなわち、ユーザはICカードを自分の使用可能な複数台のコンピュータ（例えばデスクトップPCと、ラップトップPCなど）に接続して使用することが可能である。利用履歴がコンピュータ側に記録されることを考えると、利用履歴は複数のコンピュータに分散されてしまう。従って、複数台に分散された履歴はその時間的順序は失われてしまうことになる。

【0027】利用履歴の場合には時間的な順序が非常に重要な要素となる。すなわち、複数の連続した利用履歴から、後で利用量を計算する可能性があるからである。例えば、簡単な例では利用開始時刻と利用終了時刻との差から利用時間を計算したり、利用開始時の操作対象データ長と利用終了時の操作対象データ長からデータ長の差を計算し、それを利用量としたりするなどの場合である。

【0028】DES－MACはこういった課題には本質的な解決法を与えていない。

【0029】さらに、利用履歴をユーザの管理下に置いた場合のもう一つの課題は、故意もしくは事故によって、それらの一部が失われてしまう可能性があるということである。DES－MACの場合、その一部が失われてしまうと、検証が不可能になってしまう。DES－MACでは送信者が通信の間だけ完全なデータを保持していることが前提なので、そのような場合は再送信を行えば済む。しかし、利用履歴の場合には、履歴が失われるということは本質的にデータが失われることであるので、復元は不可能である。DES－MACの方式をそのまま使用すると、残ったデータの検証さえ行うことができなくなってしまう。

【0030】さらにまた、利用量課金を行うようなシステムにおいては、ユーザの手もとに残された履歴を回収することは必須である。履歴を回収しないと、ユーザの利用料金を計算できなかったり、あるいは、回収した利用料金を情報の提供者に分配できなかったりするという問題があるからである。

【0031】従って、ユーザの手もとに残された利用履歴を安全に回収しなければならない。そのためには、偽の回収命令などによって、回収が行われてしまうようなことが無いようにしなければならない。

【0032】従って、この発明の目的とするところは、計算能力の低く、記憶容量が小さくても、高速にかつ長大なデータを検証可能な装置を提供することにある。

【0033】さらに、この発明の第二の目的は、データの順序が保存されないような環境においても、順序を復元可能な方法を提供することになる。

【0034】さらに、この発明の第三の目的はデータの一部が失われた場合でも、残ったデータの検証が可能な方法を提供することである。

【0035】さらに、この発明の第四の目的は、データを保持する装置を外部から安全に制御する方法を提供することにある。

【0036】

【課題を解決するための手段】この発明は、上記の課題を解決するために、基本的には、保持するデータ量を減らすために、データを防御装置内に記録せず、防御装置

の外に出力し、その代わりとしてデータ量の小さな検証値を防御装置内に保持するようにした。そして、具体的な構成では、高速にデータの検証を行うことができるように、電子署名の代わりに一方向性関数によって検証を行うようにした。一般にＭＤ５を代表とするハッシュ関数はＲＳＡの暗号化処理に比べるとソフトウエアで実現した場合には３桁程度ハッシュ値の方が速いという結果が出ている。また、特に、履歴データの順序を復元可能とするために、履歴データに順序を復元可能な情報を付加した。さらに、具体的には、防御装置を安全に制御するために、防御装置が保持する検証値に対して正当者の署名を付与した値が必要な構成とした。これにより防御装置内の検証値が正当者に強制的に送られ、検証の実行を確保している。

【００３７】さらに、この発明の構成について説明する。この発明によれば、上述の目的を達成するために、データ検証方法において、順次に生成される複数のデータ本体の各々について、当該データ本体と、当該データ本体に先行するデータ本体の検証値とから当該データ本体の検証値を、防御された装置の内部において、生成するステップと、一度に検証される複数のデータ本体の内の最後のデータ本体に対して生成された検証値に上記防御された装置の内部においてデジタル署名を施して署名付き検証値を生成するステップと、上記署名付き検証値を、上記防御された装置の外部に送出するステップと、上記複数のデータ本体と上記署名付き検証値とに基づいて上記複数のデータ本体を検証するステップとを実行するようにしている。

【００３８】この構成においては、検証値にデジタル署名を施せばよく計算能力が低くてもよい。また、検証は先行するデータ本体に対する検証値と今回のデータ本体と出計算されるので、１つのデータ本体と１つの検証値のみ保持できれば処理可能であり、記憶容量が小さくてもよい。

【００３９】また、この発明においては、上述の目的を達成するために、検証対象のデータを生成する被検証データ生成装置に、順次にデータ本体を生成する手段と、検証値を保持する検証値保持手段と、上記検証値保持手段において保持されている検証値と新たに生成されたデータ本体とから新たな検証値を生成し、上記新たな検証値で上記検証値保持手段に保持されている検証値を更新するする検証値生成手段と、所定のタイミングにおいて上記検証値保持手段に保持されている検証値に署名を施す署名手段とを設け、さらに上記検証値生成手段、上記検証値保持手段および上記署名手段を防御された装置内に設けるようにしてる。

【００４０】この構成においても、検証値にデジタル署名を施せばよく計算能力が低くてもよい。また、検証は先行するデータ本体に対する検証値と今回のデータ本体と出計算されるので、１つのデータ本体と１つの検証値のみ保持できれば処理可能であり、記憶容量が小さくてもよい。

【００４１】また、この発明によれば、上述の目的を達成するために、順次に生成された複数のデータ本体と、上記複数のデータ本体から計算された検証値に署名が施された署名付き検証値とを受け取る手段と、受け取った上記署名付き検証値の署名を検証する署名検証手段と、上記署名検証手段により署名の検証された検証値から、受け取った上記複数のデータ本体が正しいことを検証する検証手段とを設けるようにしている。

【００４２】この構成においては、署名の検証は署名付き検証値に対して行えばよいので、計算量を少なくすることができる。

【００４３】また、この発明によれば、上述の目的を達成するために、履歴保持方法において、複数の連続した履歴データからなる履歴データ群に対して、順次計算される唯一の検証値のみを防御された装置内に保持し、上記検証値を上記防御された装置の外部に出力する際には、上記検証値のみにデジタル署名を施すようにしている。

【００４４】この構成においても、計算量や記憶容量を抑えることができる。

【００４５】また、この発明によれば、上述の目的を達成するために、履歴保持装置に、複数の連続したデータを入力するためのデータ入力手段と、上記データを処理するためのデータ処理手段と、上記データの処理に関連する履歴データと、その時点で保持する検証値を入力として、検証値を生成するための検証値生成手段と、生成された上記検証値を保持するための検証値保持手段と、該検証値に対して署名を施すための署名手段とを設けるようにし、少なくとも上記検証値生成手段、上記検証値保持手段および上記署名手段を防御された装置内に保持するようにしている。

【００４６】この構成においても、計算量や記憶容量を抑えることができる。

【００４７】また、この構成において、上記検証値生成手段に用いる計算を一方向性関数とすることができる。また、上記履歴データの形式を、履歴データ本体とその履歴データを処理した時の検証値との組とすることができる。また、データを処理する毎にカウントするカウンタ手段をさらに設け、上記履歴データ群における履歴データの形式が、データを処理した時のカウンタの値と履歴本体からなるようにすることができる。また、利用者の出力要求に応じて、署名された検証値を出力するようにすることができる。さらに、上記履歴保持装置が単一のＣＰＵとソフトウェアで構成され、データ処理手段によるＣＰＵの負荷が低い時に上記署名手段が、適宜検証値に署名した検証値を作成して出力するようにすることができる。

【００４８】また、この構成において、データ処理手段

と、上記検証値を出力した時点で上記データ処理手段の機能を停止し、外部から正当な命令が与えられまではそデータ処理手段の機能を停止する機能停止手段とをさらに設けるようにしてもよい。また、機能を停止させるための停止条件保持手段を設け、停止条件保持手段に記述されている条件を満たした時には、上記機能停止手段が上記検証値に署名した署名付き検証値を出力して、機能を停止するようにしてもよい。さらに、外部の正当者の公開鍵を保持するための正当公開鍵保持手段を有し、上記機能停止手段が、機能を復帰させるために受け付ける命令が、最後に出力した検証値に外部の正当者が電子署名を施したものであって、上記機能停止手段が命令を受け取った時に該正当公開鍵保持手段に保持されている公開鍵で署名を検証し、さらに署名されている検証値が、上記検証値保持手段に保持されている検証値と等しいかどうかを確認するようにしてもよい。

【００４９】また、この発明によれば、上述の目的を達成するために、履歴検証装置に、複数の連続する履歴データ群とそれらのデータ群から計算された検証値に署名が施された署名付き検証値を入力するためのデータ入力手段と、入力した上記署名付き検証値の署名を検証するための署名検証手段と、入力した上記データ群と署名の検証された検証値とから、入力した上記データ群が正しいことを検証するための検証手段とを設けるようにしている。

【００５０】この構成においては、署名付き検証値に対して署名の検証を行えば済むので計算量を抑えることができる。

【００５１】また、この構成において、前回に入力した検証値を記憶するための前検証値記憶手段を設け、検証手段が検証する際に、該前検証値も用いるようにしてもよい。また、上記検証手段に用いる計算を一方向性関数としてもよい。また、上記履歴データの形式を、履歴データ本体とその履歴データを処理した時の検証値との組とすることができる。さらに、上記履歴データ群における履歴データの形式を、データを処理した時のカウンタの値と履歴本体とから構成するようにしてもよい。

【００５２】また、この発明によれば、上述の目的を達成するために、履歴保持装置に、データを保持するためのデータ記憶手段と、機能を停止する際のある一定の条件を保持するための停止条件保持手段と、該停止条件保持手段に保持された条件を満たした時に機能を停止し、外部から正当な命令が与えられるまでは機能を停止しつづけるための機能停止手段と、秘密鍵を保持するための秘密鍵保持手段と、データ保持手段に保持されたデータ群に該秘密鍵保持手段に保持された秘密鍵を用いて電子署名を施すための電子署名手段と、署名した電子署名を保持するための電子署名保持手段と、外部の正当者の公開鍵を保持するための正当公開鍵保持手段とを設け、上記機能停止手段が機能を復帰させるために受け付ける命令が、上記電子署名保持手段に保持された電子署名に対して外部の正当者が電子署名を施したものであって、機能停止手段が命令を受け取った時に該正当公開鍵保持手段に保持されている公開鍵で署名を検証し、さらに署名されている値が、電子署名保持手段に保持されている値と等しいかどうかを確認するようにしている。

【００５３】この構成においては、履歴の正当性が検証されて初めて正当者の署名した命令が送付され、この正当な命令が検証されて初めて装置の停止状態が解除される。従って、正当な履歴が回収されないままでサービスが提供され続けるという不都合がない。換言すると、正当な履歴の回収が確保される。

【００５４】また、この発明によれば、電子機器に、所定の条件が満たされたときに電子機器本体の少なくとも一部の機能を停止する機能停止手段と、所定のデータを外部に出力する手段と、上記所定のデータに署名を施して生成された署名付きデータを受信する手段と、上記署名付きデータについて署名を検証する署名検証手段と、上記署名検証手段によって上記署名付きデータの署名の正当性が検証されたときに上記一部の機能の停止を解除する手段とを設けている。

【００５５】この構成においては、データの正当性が確認されて初めて電子機器の使用が継続できる。従って正当なデータを確保することができる。

【００５６】また、この発明は、その一部をコンピュータプログラム製品として実現することができる。

【００５７】

【発明の実施の態様】

［第１の実施例］以下、この発明の実施例について説明する。まず第１の実施例について説明する。この実施例も後述する他の実施例も、暗号化されて流通しているプログラムや画像情報などのデジタル情報一般を、パソコンやワークステーションなどの情報処理装置上で利用し、その際の利用履歴をその情報処理装置に接続したＩＣカード（以下、トークンと呼ぶ）において、情報を復号するタイミングをとらえて記録し、その利用履歴をセンターが回収するというシステムである。もちろん履歴データのセキュリティ確保以外にもこの発明を適用することができる。

【００５８】図１は、この実施例の全体的な構成を示す。図１において、利用者の環境にはパソコンやワークステーションなど、デジタル情報を利用するための情報処理装置１１があり、それには暗号化された情報を復号する（あるいは復号するための鍵を復号する）ため、およびそのタイミングを捕らえて利用履歴を記録するためのトークン１２が接続されている。トークン１２と情報処理装置１１の間の接続は、ＰＣカード（ＰＣＭＣＩＡ：パーソナル・コンピュータ・メモリ・カード・インターフェース・アソシエーション）インターフェース、シリアル、パラレル、赤外線など、情報を伝達できる手

段であれば何でも用いることができる。情報処理装置１１の内部に実装するようにしてもよい。

【００５９】ユーザの情報処理装置１１はセンター側の、ワークステーションあるいは大型計算機などの情報処理装置で構成される回収装置１３と必要に応じて接続される。接続の形態は、モデムと電話回線、あるいはイーサネットなどのネットワークインターフェースでよい。この接続は常時行われる訳ではなく、利用者の情報処理装置１１から利用履歴の回収が必要な時のみ行われれば十分である。

【００６０】図２にユーザ側の情報処理装置１１の構成を示す。ユーザの情報処理装置１１は一般のパソコンやワークステーションで良い。トークン１２が接続されているところのみが異なる。情報処理装置１１は、制御部１４、情報保持部１５、履歴保持部１６および履歴送信部１７を実現する。このような構成は、例えばプログラムが記録された記録媒体１１ａを用いて当該プログラムをインストールすることにより実現できる。

【００６１】制御部１４はトークン１２と通信しながら、以下のような処理を行う。

①情報保持部１５に格納されている暗号化された情報を読み出し、トークン１２へ渡して復号してもらい、復号された情報を実行あるいは処理する。

②復号データを受け取った際に同時にトークン１２から渡される利用履歴を受け取り、それを履歴保持部１６に格納する。

③ユーザからの指示を受けて、トークン１２に「検証値出力」の命令を出し、その結果である電子署名の施された検証値を履歴送信部１７に渡す。

【００６２】情報保持部１５は利用者が利用するデータや情報、あるいは暗号化されたデータが格納されている。実際にはメモリあるいはハードディスク装置などの外部記憶装置で構成される。

【００６３】履歴保持部１６は制御部１４を通じてトークン１２側から渡された履歴が格納される。実際にはメモリあるいはハードディスク装置などの外部記憶装置で構成される。履歴の具体的な構成については後述する。

【００６４】履歴送信部１７は制御部１４からの命令を受けて、制御部１４から渡された検証値と共に履歴保持部１６に保持されている履歴を読み出して、センターの回収装置１３に送信する。実際にはモデムと電話回線、あるいはイーサネットなどのネットワークインターフェースなどで構成される。あるいは、ネットワークでなくともフロッピーディスクなどの装置へ一旦格納し、それをユーザが人手でセンターの回収装置１３に入力するようにしてもよい。

【００６５】図３にユーザ側のトークン１２の構成を示す。トークン１２は物理的には一般のＭＰＵ、メモリ等から構成される。トークン１２はそれ自体が、メモリの内容を読み出したり破壊したりするなど、外部からの物理的な攻撃に耐えるように攻撃対抗容器内に収められる。攻撃対抗容器は周知の技術であるので（特許第１８６３５３号、特許第１８６０４６３号、特開平３－１００７５３号公報等）、ここでは説明を省略する。なお、どの程度の攻撃に耐えうるものを選ぶかはデータのセキュリティの程度に応じて変化する。攻撃態勢が弱いものでもよい場合もある。

【００６６】トークン１２はユーザの情報処理装置１１に接続され、情報処理装置１１からの指示に従って一定の処理を行い、その結果を返す。トークン１２はユーザ秘密鍵保持部１８、復号部１９、検証値生成部２０、検証値保持部２１、検証値出力部２２、トークン秘密鍵保持部２３、電子署名部２４等を有している。トークン１２の各構成部については後に詳述する。トークン１２は以下の機能を持つ。

【００６７】①情報の復号機能と利用履歴の保持

（１）情報処理装置１１から暗号化データを受け取り、それをユーザ秘密鍵保持部１８に格納されている秘密鍵で復号し、復号データを情報処理装置１１に返す。

（２）復号処理を行うと同時に復号されたデータのヘッダを参照し、そこに記されている情報識別子を参照し、その識別子を利用履歴として情報処理装置１１に返す。

（３）さらに、利用履歴は検証値生成部２０にも渡され、検証値生成部２０は利用履歴とその時点で検証値保持部２１に保持している検証値とに対して計算を行い、その計算結果を検証値保持部２１に格納する。

【００６８】②検証値の出力機能

情報処理装置１１からの出力要求を受けて、その時点で検証値保持部２１に保持している検証値に電子署名を施して返す。その後、検証値保持部２１内のデータを消去する。

【００６９】以下、トークン１２の各構成部について説明する。

【００７０】復号部１９は情報処理装置１１からの復号要求に答えて、渡された暗号化データを、ユーザ秘密鍵保持部１８に保持されているユーザ固有の秘密鍵を用いて復号処理を行い、その結果を復号データとして情報処理装置１１側へ返す。このとき、それと同時に復号したデータのヘッダを読み取り、そこに記されている情報識別子を利用履歴として情報処理装置１１側へ返すと共に、検証値生成部２０にも渡す（この例では利用履歴は、利用した情報の情報識別子を用いている）。

【００７１】このように構成することで、ユーザは情報を利用する際には必ずトークン１２へのアクセスが必要となり、利用履歴を確実に記録することができるようになる。

【００７２】ここで、情報処理装置１１側から渡される暗号データは、情報そのものが暗号化されたものでもよいし、あるいは暗号化された情報を復号するための鍵を暗号化したものでもよい。後者の場合には情報処理装置

１１側で情報本体の復号処理がなされることになる。

【００７３】ユーザ秘密鍵保持部１８は、ユーザ固有の秘密鍵を保持する。一般的には、トークン１２は予めトークン発行センターなどによって、ユーザごとの固有の鍵を封入した形でユーザに配布される。従って、このユーザ秘密鍵はユーザ自身も知ることができない。

【００７４】検証値保持部２１は順次更新される一つの検証値のみを保持する。検証値は一般に１６バイトなど、固定の長さを持つ値である。従って、検証値が１６バイトであるならば、１６バイトのメモリだけで構成される。図４に検証値の構成例を示す。

【００７５】検証値出力部２２は、情報処理装置１１側からの検証値の出力要求を受けて、その時点で検証値保持部２１に格納されている検証値を読み出し、それを情報処理装置１１側に返すという機能を持つ。その際、検証値出力部２２は電子署名部２４を呼び出して、検証値に対して電子署名を施す。

【００７６】電子署名部２４はそのトークン専用の秘密鍵を保持するトークン秘密鍵保持部２３に保持された秘密鍵を用いて、与えられた値に対して電子署名を施す処理を行う。トークン秘密鍵保持部２３は電子署名を行う際に用いられる署名用の秘密鍵を保持する構成部である。これらの構成部にはＲＳＡ署名などの電子署名技術を用いることが可能であり、従来の技術であるのでここでは詳細な説明は省略する。

【００７７】検証値生成部２０は復号部１９から利用履歴（ここでは情報識別子）を受け取ったら、検証値保持部２１に保持されている検証値を読み取り、利用履歴と検証値とから、以下のような計算を行って新しい検証値を計算する。

【００７８】

【数１】Ｈ＝Ｈａｓｈ（Ｕｓａｇｅ＋Ｈｏｌｄ）

ここで、Ｈは新しい検証値、Ｈｏｌｄは現在の検証値、Ｕｓａｇｅは利用履歴、Ｈａｓｈ（）は一方向性関数を意味し、実際にはＭＤ５やＳＨＡ（ＳｅｃｕｒｅＨａｓｈ　Ａｌｇｏｒｉｔｈｍ）などが用いられる。この演算における”＋”という演算は実際に数値として足し算を行ってもよいし、長さが同じであれば排他的論理和を取っても、あるいは、単に二つのデータを順に並べただけでもよい。いずれにしろ二つの値を合成したものであればよい。検証値生成部２０はこのように計算した新しい検証値を、検証値保持部２１に格納する（つまり、古い値を上書きする）。

【００７９】検証値出力部２２は情報処理装置１１からの出力要求を受け、その時点で検証値保持部２１に保持している検証値を返してから、検証値保持部２１を予め決められた値に初期化するようにする。あるいは単純にクリアするようにしてもよい。

【００８０】次にセンターの回収装置１３について説明する。回収装置１３の構成を図５に示す。図５において、回収装置１３は、履歴受信部２５、履歴保持部２６、履歴検証部２７、トークン公開鍵保持部２８、署名検証部２９等を有している。回収装置１３はユーザの情報処理装置１１から送られた履歴を履歴受信部２５によって受信し、その内容を履歴保持部２６に格納する。格納された利用履歴は履歴検証部２７によって読み取られ、履歴が正しいかどうかが検証され、その結果はセンター側の管理者に出力される。

【００８１】一般的にはセンターはこの後、その履歴の内容に従って、情報の利用料金を計算し、その料金を利用者から徴収し、徴収した利用料金を情報の利用履歴の明細に従って、情報提供者に分配するという処理を行う。しかし、本発明の本質とは直接は関係無いのでここでは説明を省略する。

【００８２】以下、回収装置１３の各構成部について説明する。

【００８３】履歴受信部２５は情報処理装置１１から送られてくる履歴情報を受信する。実際には情報処理装置１１の履歴送信部１７（図２）と同様にモデムと電話回線あるいはイーサネットなどのネットワークインターフェース、あるはフロッピーディスク装置などの外部からの情報入力装置で構成される。履歴受信部２５によって受信された利用履歴は履歴保持部２６に格納される。

【００８４】さらに、情報処理装置１１から送られてきた検証値が正当なものであるかどうかを検証するために、トークン公開鍵保持部２８と署名検証部２９を有している。

【００８５】情報処理装置１１から履歴が送信されると、履歴受信部２５が受け取る。受け取った履歴は履歴保持部２６に格納されると共に、署名検証部２９に渡される。署名検証部２９はトークン公開鍵保持部２８に格納されている複数のトークン公開鍵の中から履歴を送信してきた情報処理装置１１に接続されているトークン１２の公開鍵を選択し、その公開鍵を用いて履歴の署名を検証する。その検証結果は履歴保持部２６に格納されている履歴とともに保持される。もし、検証結果が偽であるという結果が出た場合にはその検証値は改竄あるいは偽造された可能性があるので、以下の処理は続行せず、管理者にその旨のメッセージを出力して処理を停止する。

【００８６】署名が検証された場合は以下の処理が続けられる。

【００８７】履歴保持部２６は履歴受信部２５から渡された利用履歴および検証結果を保持する。履歴保持部２６は実際にはメモリなどの記憶装置で構成される。

【００８８】履歴検証部２７は履歴保持部２６に保持された履歴を以下のようにして検証する。

（１）送信された履歴の系列を、ud_1，ud_2，ud_3．．．ud_nとする。

（２）履歴の最後に添付されている検証値を、ｈｕｄと

する。
（3）検証値の初期値をihudとすると、以下の計算式に従って、計算した結果であるhud'が、送られてきたhudと等しくなるかどうかを調べる。
【0089】
【数2】hud'=Hash(ud_n+Hash(ud_{n-1}+...Hash(ud_2+Hash(ud_1+ihud))...))
hud=?hud'
（4）もし等しければ、改竄されていない、等しくなければ改竄されていると判断し、その結果を回収装置の管理者に通知する。
【0090】次に各部で処理される情報の形式について説明する。
【0091】図6にトークン12で復号の対象となる暗号化された情報の形式を示す。（a）は情報そのものをユーザの秘密鍵で暗号化している場合である。（b）は、最初に情報本体を暗号化するのに用いている秘密鍵をユーザ固有の秘密鍵で暗号化したものを復号し、その結果得られた情報固有の秘密鍵を用いて、情報本体の復号を行うという場合である。（b）の場合には情報本体の復号はトークン12ではなく、情報処理装置側で行ってもよい。また、ここでは慣用暗号を用いている例を説明しているが、これらは公開暗号を用いてもよいことは言うまでもない。
【0092】ここで、情報識別子とは、センターが情報を暗号化させて流通させる時に付与される情報固有の識別子である。情報識別子はセンターによって管理され（データベースを持つなどによって）、情報識別子を特定すると、その情報が誰によって作成されたものであるのか、などを特定できる。
【0093】図7には利用履歴の形式を示す。（a）は本実施例における情報処理装置11内に記録される利用履歴であり、利用した（トークンで復号した情報の）情報識別子の列である。（b）は情報処理装置11からセンターに送付される利用履歴であり、（a）の最後にトークンが保持する検証値、および検証値に対するトークンの署名が添付されているところのみが異なる。
【0094】個々の利用履歴は本実施例では利用した情報識別子のみで構成されているが、これは任意のデータ、例えば、利用した時刻、利用者の識別子、利用量、利用金額などが含まれていてもよい。すなわち種々の情報を履歴として残す場合（一般に履歴は種々の情報を残すのが一般的である）には個々の履歴が長くなるため、本発明が有効となる。
【0095】次に情報処理装置11およびトークン12における処理を図8から図12を参照して説明する。図8は情報処理装置11の制御部14において、利用者から情報の利用要求が有った時の処理の流れである。図9は同じく制御部14において利用者から利用履歴回収命令が有った時の処理である。図10はトークン12の復号部19が情報処理装置11から暗号化された情報の復号要求を受け取った時の処理である。図11はトークン12の復号部19から呼び出されるトークン12の検証値生成部20の処理である。図12はトークン12の検証値出力部22が情報処理装置11から検証値出力要求を受け取った時の処理である。
【0096】図8に示すように、利用者から情報利用の要求があったときには情報処理装置11の制御部14においてつぎのように処理が進む。まず、対象の情報が暗号化されているかどうかを判別し（S11）、暗号化されていなければ情報をそのまま処理する（S15）。暗号化されているときにはトークン12に対して復号要求を出して、対象情報を引き渡す（S12）。このとき、トークン12からエラーが返されたら「トークンの履歴が一杯です」というエラーメッセージを出して処理を終了する（S13、S16）。エラーが返されなければ、トークン12から過関された利用履歴をディスク等の記録装置に記録する（S14）。そして対象情報を処理する（S15）。
【0097】図9に示すように、利用者から利用履歴回収命令があったときには情報処理装置11の制御部14においてつぎのように処理が進む。まず、対象の情報が暗号化されているかどうかを判別し（S21）、暗号化されていなければ情報をそのまま処理する（S24）。暗号化されているときにはトークン12に対して復号要求を出して、対象情報を引き渡す（S22）。そしてトークン12から返された利用履歴をディスク等の記録装置に記録する（S23）。こののち対象情報を処理する（S24）。
【0098】図10に示すように、トークン12の復号部19が情報処理装置11から暗号化された情報の復号要求を受け取った時にはつぎのように処理が進む。まず、ユーザ秘密鍵保持部18からユーザ秘密鍵Kuが取り出される（S31）。暗号化データをユーザ秘密鍵Kuで復号して復号データを記憶する（S32）。復号データのヘッダを参照して情報識別子を読み取り、この識別子を引数として検証値生成部20を呼び出し検証値生成処理を実行させる（S33、S34、図11参照）。この後復号データと識別子とを情報主おりそう値35に返す（S35）。
【0099】図11に示すように、トークン12の検証値生成部20がトークン12の復号部19から呼び出されたときにはつぎのように処理が進む。まず、検証値保持部21から検証値を取り出す（S41）。情報識別子と検証値とについてハッシュ計算を行って、計算結果を新たな検証値として検証値保持部21に記憶する（S42、S43）。
【0100】図12に示すように、トークン12の検証値出力部22が情報処理装置11から検証値出力要求を

受け取った時にはつぎのように処理が進む。まず、検証値保持部２１に記憶されている検証値を読み出す（Ｓ５１）。こののち、検証値保持部２１の記憶内容を初期化する（Ｓ５２）。読み出した検証値を引数として電子署名部２４を呼び出し、検証値に署名を施す（Ｓ５３）。検証値の後に署名を付して出力する（Ｓ５４）。

【０１０１】以上で第１の実施例の説明を終了する。

【０１０２】なお、特願平８－６２０７６号のユーザ認証装置および方法を、本発明と組み合せて使用した場合には、発行するアクセスチケットごとにべき乗剰余の計算における法ｎを変えるようにすることで、法ｎを情報識別子として用いることができる。すなわち、特願平８－６２０７６号のユーザ認証手法ではアクセスチケット（認証用補助情報）を外部から受け取り、このアクセスチケットとユーザ識別情報とを用いて証明、例えば暗号データの復号を行うようになっている。そして、このときに用いる法ｎを情報識別子として利用する。その場合には、法ｎはトークンの内部の復号装置で復号されてから取り出されるのではなく、復号対象の情報と共に外部から与えられることになる。

【０１０３】このように構成することで、トークン１２内部に用意しなければならない検証値保持部２１の容量を最小に押さえることができ、トークン１２の生産コストを低くすることが可能となる。

【０１０４】［第２の実施例］次に本発明の第２の実施例について説明する。ここで述べる実施例は第１の実施例に対して、幾つかの機能を追加したものである。以下にその機能と効果について列挙する。

【０１０５】①トークン１２が検証値を出力して機能を停止し、センターからメッセージを受け取ると機能を回復する。

【０１０６】検証値を外部に出力する時やあるいは時計機能を用いて一定時間を経過した時などに、利用者に履歴の回収を促すためにトークン１２がその時点での検証値を出力して停止するようにする（あるいは自律的に停止して検証値を要求するようにしてもよい）。利用者がトークン１２の機能を回復させるためにはセンターに履歴と検証値を送信して、確認してもらい、センターから機能を回復させるためのメッセージを受け取るしかない。センターが発行する機能回復用のメッセージは、ユーザから送られた検証値にセンターが電子署名を施したものとする。

【０１０７】②履歴としてその利用履歴を処理した時点での検証値も出力する。

【０１０８】利用履歴の内容を情報識別子だけではなく、その履歴を生成した時点での検証値も含ませる。これによって、個々の履歴の連続性を後から調べることが可能になり、情報処理装置側での履歴の（順序の）管理を厳密に行わなくても良いようにする。

【０１０９】③センター側で古い検証値を保持する。

【０１１０】これまでの実施例では、利用者からの出力要求によって、トークン内部の検証値は初期化されていた。しかしながら、センターの回収装置側で利用者の前回の検証値を保持することによって、その機能を不要にすることができる。

【０１１１】図１３に本実施例におけるトークン１２の構成を示す。なお、図１３において図３に対応する箇所には対応する符号を付して詳細な説明を省略する。この図において、トークン１２は、ユーザ秘密鍵保持部１８、復号部１９、検証値生成部２０、検証値保持部２１、トークン秘密鍵保持部２３、電子署名部２４、制御部３０、履歴生成部３１、計数部３２、センター公開鍵保持部３３、署名検証部３４等を有している。なお、必要に応じて時計部３５を設けてもよい。

【０１１２】本実施例では情報処理装置１１との通信はすべて制御部３０を介して行われるように構成され、制御部３０は情報処理装置１１からの要求に対し適切に他の処理部を呼出して処理を行う。

【０１１３】制御部３０はその内部にトークン１２の動作状態を保持しており、動作状態には通常モードと停止モードの二つのモードがある。通常モードにおいてはトークン１２は情報処理装置１１からの復号要求に対して、第１の実施例で述べたように復号処理を行い、その結果を返すという処理を行う。一方、停止モードにおいては復号要求の処理は受け付けない。停止モードにおいては基本的には機能再開要求（センター署名付き検証値）のみを受け付け、その要求が正当である場合には停止モードを解除し、通常モードへ移行するという処理を行う（実際にはそれ以外にもその時点で検証値保持部２１に保持している検証値に署名した検証値を出力するという処理も受け付けるようにしてもよい）。

【０１１４】通常モードから停止モードへの移行は、例えば復号処理を行った回数などによる。図１３の計数部３２は復号処理を行った回数を保持している。例えば、その回数が予め定められた回数（例えば１００回など）を超えたら、「期限が過ぎた」旨のメッセージを情報処理装置１１側に返して、停止モードへ移行する。

【０１１５】構成として時計を有する場合には、制御部３０内部に保持された前回の停止時刻の情報に基づいて行うようにしてもよい。すなわち、制御部は情報処理装置からの要求があったとき、制御部内に保持された前回停止時刻と現在の時刻を比較し、予め決められた時間（例えば一か月、など）が経過していた場合には「期限が過ぎた」旨のメッセージを情報処理装置１１側に返して、停止モードへ移行する。

【０１１６】つぎにトークン１２の制御部３０の処理を図１４～図１６を参照して詳細に説明する。なお、図１４～図１６において点線で示してある箇所は制御部３０の処理ではなく、関連する構成部の処理であることを意味する。

【0117】図14において、情報処理装置11からトークン12の制御部30に復号要求、検証値出力要求および機能再開要求のいずれかが入力される。まず、制御部30のモードが停止モードかどうかが判別される（S61）。停止モードでないときには計数部32の計数値が読み取られ、この計数値が基準値、例えば100を越えたかどうかが判別される（S62、S63）。100を越えていない場合には図16のノードBに進み、復号処理等を行う。100を越えている場合には署名付き検証値を出力する。すなわち、検証値保持部21の値を読み出し、電子署名部24により署名付き検証値を生成させ、受け取る（S64、S65）。こののち、署名付き検証値と「停止モードへ移行」というメッセージを情報処理装置11に返す（S66）。そして計数部32の計数値をクリアして停止モードに移行する（S67、S68）。

【0118】ステップS61において、制御部30が停止モードの場合には、受け取った要求が復号要求か、検証値出力要求か、機能再開要求かが判別される（S69、S70、S71）。要求が復号要求の場合には情報処理装置11に「現在は停止モードである」というメッセージを返し、処理を終了する（S72）。要求が検証値出力要求の場合には検証値保持部21の検証値を読み取り、電子署名部24により署名付き検証値を生成させ、受け取る（S73、S74）。こののち、署名付き検証値を情報処理装置11に返し処理を終了する（S75）。機能再開要求のときには図15のノードAの機能再開処理に進む。受け取った要求が復号要求、検証値出力要求、機能再開要求のいずれでもない場合には情報処理装置11にエラーを返して処理を終了する（S76）。

【0119】図15は機能再開処理を示す。図15において、まず、受け取ったセンター署名付き検証値を署名検証部24に渡して署名の正当性を検証する（S77）。署名が正しければ、渡された検証値と、検証値保持部21の検証値とを比較し、双方が一致するかどうかを検査する（S78～S80）。一致すれば制御部のモードを停止モードから通常モードに移行させ、「機能再開」のメッセージを情報処理装置11に返す（S81、S82）。ステップS78において署名が正しくない場合には、「署名が正しくない」というメッセージを情報処理装置11に返して処理を終了する（S83）。ステップS80において検証値が一致しない場合には「検証値が正しくない」というメッセージを情報処理装置11に返して処理を終了する（S84）。

【0120】図16は計数値が閾値例えば100を上回っていない場合の処理を示す。図16において、まず要求が復号要求かどうかが検査される（S85）。復号要求の場合には渡されたデータを復号部19に送る（S88）。復号部19は復号を行う（S89～S93）。また要求が復号要求でない場合には検証値要求かどうかが判別される（S86）。検証値要求である場合には図14のノードCに進み、検証値出力処理を行う。ステップS86において検証値出力要求でもない場合にはエラーを情報処理装置11に返して処理を終了する（S87）。

【0121】以上でトークン12の制御部30の処理の説明を終える。

【0122】なお、この例では、情報処理装置11側から検証値要求が有った時にも停止モードへ移行するようにしているけれども（図16のステップS86から図14のノードCへ移行）、そうしなくても構わない。例えば通常モードにおける検証値要求に対しては、検証値を更新して単にその時点で保持している検証値に署名した値を返すようにしてもよい（このメリットについては本実施例の説明の最後で述べる）。

【0123】復号部19、ユーザ秘密鍵保持部18は第1の実施例と同様の機能を有する。

【0124】履歴生成部31は図16でも示したように復号部19から渡された情報識別子と現在の検証値の三つの組を生成し、それを利用履歴として制御部30に渡すという処理を行う。

【0125】検証値生成部20は履歴生成部31から渡された履歴udに対し、

【0126】

【数3】Hu＝Hash（ud）

なるハッシュ値を計算し、それを検証値保持部21に格納するという処理を行い、検証値保持部21はその時点での検証値を保持する。

【0127】電子署名部24は第1の実施例と同様に、そのトークン専用の秘密鍵を保持する秘密鍵保持部23に保持された秘密鍵を用いて、与えられた値に対して電子署名を施す処理を行う。本実施例ではさらに、署名検証部34が設けられ、センター公開鍵保持部33に保持されたセンターの公開鍵を用いて渡された署名がセンターの署名であるかどうかを検証するという処理を行う。これらの構成部には基本的にはRSA署名などの電子署名技術を用いることが可能であり、周知の技術であるのでここでは詳細な説明は省略する。

【0128】本実施例における情報処理装置11の構成を図17に示す。図17において図2と対応する箇所には対応する符号を付す。この図において、基本的には第1の実施例のものとほぼ同じ構成であるが、本実施例の情報処理装置11ではある時点でトークンが停止モードに入ってしまうので、それを再開させるためにはセンターに履歴を送信し、それに対する再開メッセージを送ってもらわねばならない。そこで、センターからの署名付きの検証値を受け取る署名付き検証値受信部36があるところが異なる。また、履歴保持部16に保持される履歴の構成が異なっている。

【0129】図18に本実施例におけるセンターの回収装置13の構成を示す。図18において図5と対応する箇所には対応する符号を付す。この図において、構成としては第1の実施例のものに比べると、履歴の正当性が検証された場合には情報処理装置11にセンターの署名付き検証値を送らねばならないので、それを行うための構成部、すなわちセンター秘密鍵保持部37、電子署名部38、署名付き検証値送信部39が増設されている。また、情報処理装置11側から送られる利用履歴の構成が異なっているので、当然回収センターで処理される履歴も異なる。

【0130】図19に各部で保持される利用履歴の構成を示す。（a）は情報処理装置11の履歴保持部16に記録される利用履歴である。個々の履歴の内容は（c）に示されたような情報識別子とその時点でトークンに保持されていた検証値のペアの構成となっている。

【0131】情報処理装置11からセンターに履歴を送付する際には、その履歴の列の最後にトークン12の署名の付いた検証値が付与される（b）。署名付き検証値はトークン12が機能を停止した際に出力されるものであり、その時点での検証値にトークン12が電子署名を施したものである（d）。

【0132】センターは履歴の検証のために（d）の署名付き検証値を用いる。そして検証の結果、正当なものであると判断されると、トークン12の機能を再開させるためのメッセージとして最後に添付された検証値にセンターが電子署名を施した値を情報処理装置11に送る。それが（e）である。

【0133】次に回収装置13の処理について説明する。情報処理装置11から履歴が送信されると、履歴受信部25が受け取る。受け取った履歴は履歴保持部26に格納されると共に、署名検証部29に渡される。署名検証部29はトークン公開鍵保持部28に格納されている複数のトークン公開鍵の中から履歴を送信してきた情報処理装置11に接続されているトークン12の公開鍵を選択し、その公開鍵を用いて履歴の署名を検証する。その検証結果は履歴保持部26に格納されている履歴とともに保持される。

【0134】履歴の受信が終わると履歴検証部27が動作しはじめる。履歴検証部27は今受信した履歴を参照し、それに付随している署名の検証結果を参照する。署名の検証結果が正当でない場合には、これ以降の処理は行われない。履歴に付随している検証結果が正当であれば、さらに履歴の内容が正当であるかどうかを検証する。

【0135】履歴の内容の検証処理は以下のように行われる。

（1）送られてきた履歴の列が以下のようなものであるとする。

(id_1, hu_0), (id_2, hu_1), (id_3, hu_2), ..., (id_n, hu_{n-1}), sign(hu_n)

ただし、ここでidは情報識別子、huはその履歴が生成された時点での検証値、sign()はトークンのサインであるとする。

（2）トークンが前回送ってきた際の検証値を履歴保持部の中から捜し出し、それをHuoldとする。

（3）送られてきた利用履歴の最初の履歴（ID_1, hu_0）の中から検証値hu_0を取り出し、それがHuoldと等しいかどうかを確かめる。

（4）次にHash（id_1, hu_0）を計算し、それがhu_1になるかどうかを確かめる。

（5）以下同様にして最後の検証値hu_nまで確かめる。

（6）すべての検査にパスしたら利用履歴は正当なものであると判断する。

【0136】検証処理の結果、履歴が正しいものと判断された場合のみ、最後の検証値hunが電子署名部に送られ、センターの秘密鍵で電子署名が施される。そして、センターの署名付きの検証値が履歴を送付してきた情報処理装置に送り返される。

【0137】以上のように構成することで、ある時点でトークンが機能を停止するため、その情報処理装置の利用者はトークンの機能を再開させるためには正当な履歴をセンターに送付しなければならなくなる。従って、履歴の回収を利用者に促すことが可能になる。

【0138】また、センター側に最後の検証値が記録されているため、トークンから送付された正しい履歴が何らかの理由で一部が破壊されていた場合でも、単に検証が成功しなかっただけであるので、センター側の保持データは何も変化しない。従って、その場合にはトークンが履歴を再送付すれば検証は正常に行われることになる。

【0139】また本実施例において、トークンが自律的に検証値を出力するように構成することで、回収装置側で履歴を検証する際に、一部の履歴が壊れていた（失われていた）場合でも、他の部分のほとんどについては検証可能なようにすることができる。

【0140】すなわち、前述したように利用者が検証値を要求した時だけでなく、トークンの負荷が低いときにトークンが自律的にその時点で保持している検証値に署名したものを出力することによって、回収装置側で履歴を検証する際に、一部の履歴が壊れていた（失われていた）場合でも、他の部分のほとんどについては検証が可能になる。

【0141】この場合には、センターへ送付される利用履歴は例えば図20のような構成になる。この時、何らかの事故によって情報処理装置側で履歴25が失われてしまったとする。

【0142】先に示したような検証値を最後にしか持た

ないような利用履歴の場合には履歴２６以降は検証可能となるが、履歴１から履歴２４については内容が失われていないにもかかわらずそれが正当であることは検証できない。

【０１４３】それが途中に署名付の検証値を挿入することによって、この例の場合には履歴２５が失われた場合には履歴２４のみが検証不可能となるだけで、残りの履歴については検証可能となるのである。つまり、履歴１から履歴１０までは署名付き検証値１によって、履歴１１から履歴２３までは署名付き検証値２によって、履歴２５から履歴３６までは署名付き検証値３によって、履歴３７から履歴５７までは署名付き検証値４によって、それぞれが検証可能となるからである。

【０１４４】このように適当な間隔で署名付きの検証値を履歴中に挿入することで履歴の一部が失われた場合にでも残りの履歴の大部分について検証を可能とすることができるようになるのである。

【０１４５】これを実現するためにはトークン内部の制御部において負荷が低いかどうかを判定する装置を設け、トークンの負荷が低い場合には自律的に署名付き検証値を生成しておくようにすればよい。

【０１４６】また、トークンが自律的に行わなくても情報処理装置すなわち利用者からの要求によって署名付き検証値を出力するように構成すればよい。そのためには図１６のノードＣを図１４のノードＣ（ステップＳ６４）に分岐させるのではなく、検証値を更新して署名付き検証値を生成しそれを情報処理装置１１に返すように処理を変更すればよい。

【０１４７】また、トークンに時計機能を持たせることによって、利用履歴として時刻の情報を取ることができるようになる。それによって、回収センター側は単にどの情報を利用したのかという履歴だけではなく、利用した時刻も知ることができるようになる。時計部は通常の時計機能であり、年月日および時刻を保持し、要求に従って現在の時刻を出力する機能を有するだけでよい。履歴に時刻を含ませるには、前述してきた情報識別子に時刻の情報も結合するだけでよい。また、時計機能を有すると、前述した停止モードへの移行の条件として、「前回に停止した時から経過した時間」にすることが可能になる。

【０１４８】さらにまた、本実施例では外部に出力する履歴にその時点で保持していた検証値を付与するように構成しているが、これはトークン内部にカウンタ部を設け、履歴を出力するごとにカウンタの値をカウントしていくようにし、履歴を外部に出力する際に検証値ではなく、カウンタの値を出力するようにしてもよい。その場合は、これまでの説明中のハッシュ関数の入力となる部分が、利用履歴およびその時点で保持しているカウンタの値となる。

【０１４９】

【発明の効果】以上説明したように、この発明によれば、保持するデータ量を減らすために、データを防御装置内に保管せず、防御装置の外に出力し、その代わりとしてデータ量の小さな検証値を防御装置内に保管するようにしている。したがって防御装置の記憶容量や必要処理能力を抑えることができる。検証値は署名を付して外部に送られるので改竄を防止でき、データの検証を確実に行える。また、データの順序を復元可能とするために、データに順序復元用の情報を付加することにより、分散して保管されているデータであってもその順序を復元して、検証を容易にすることができる。さらに、防御装置が保持するデータに対して正当者の署名を付与した値を、防御装置が受け取ったときに、関連する処理を継続実行できるようにしているので、継続実行するには、防御装置内に保持したデータを正当者に送り署名を受けた後返送してもらわなければならない。したがって、正当者には必然的に検証対象のデータが送られてきて、検証対象のデータを確実に回収することができる。また、署名付き検証値を頻繁に出力するようにすればデータの一部が破損等しても他の多くのデータについては確実に検証を行うことができる。

【図面の簡単な説明】

【図１】　この発明の第１の実施例を全体として示すブロック図である。

【図２】　図１の情報処理装置１１の構成を示すブロック図である。

【図３】　図１のトークン１２の構成を示すブロック図である。

【図４】　図３の検証値保持部２１を説明する図である。

【図５】　図１の回収装置１３の構成を示すブロック図である。

【図６】　トークン１２において復号される情報を説明する図である。

【図７】　利用履歴の構成を説明する図である。

【図８】　利用者から情報の利用要求が有った時の情報処理装置１１の制御部１４の処理を説明するフローチャートである。

【図９】　利用者から利用履歴回収命令が有った時の情報処理装置１１の制御部１４の処理を説明するフローチャートである。

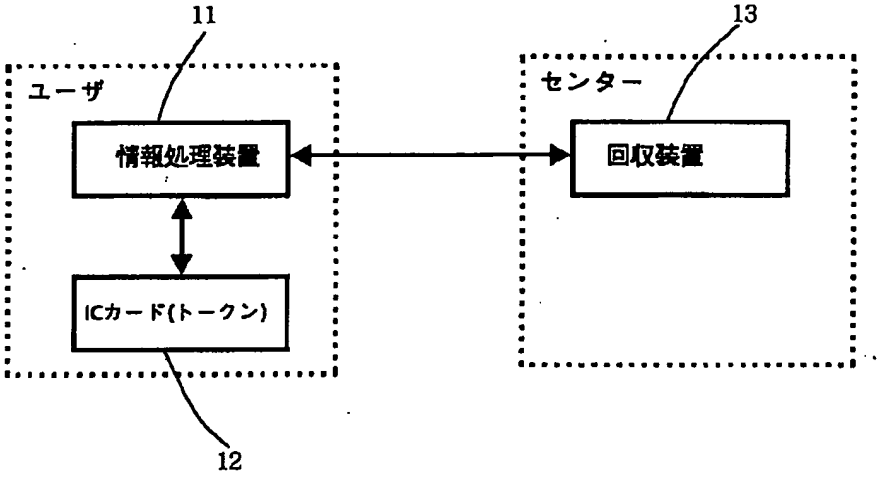
【図１０】　トークン１２の復号部１９が情報処理装置１１から暗号化された情報の復号要求を受け取った時の処理を説明するフローチャートである。

【図１１】　トークン１２の復号部１９から呼び出されるトークン１２の検証値生成部２０の処理を説明するフローチャートである。

【図１２】　トークン１２の検証値出力部２２が情報処理装置１１から検証値出力要求を受け取った時の処理を説明するフローチャートである。

【図13】　第2の実施例のトークン12の構成を示すブロック図である。
【図14】　図13のトークン12の処理を説明するフローチャートである。
【図15】　図13のトークン12の処理を説明するフローチャートである。
【図16】　図13のトークン12の処理を説明するフローチャートである。
【図17】　第2の実施例の情報処理装置11において実現されている機能ブロックを示すブロック図である。
【図18】　第2の実施例の回収装置13の構成を示すブロック図である。
【図19】　第2の実施例の利用履歴の構成を説明する図である。
【図20】　第2の実施例の利用履歴の他の構成を説明する図である。
【図21】　関連技術を説明する図である。
【符号の説明】
11　　情報処理装置
12　　トークン
13　　回収装置
14　　情報処理装置11の制御部
15　　情報処理装置11の情報保持部
16　　情報処理装置11の履歴保持部
17　　情報処理装置11の履歴送信部
18　　トークン12のユーザ秘密鍵保持部
19　　トークン12の復号部
20　　トークン12の検証値生成部
21　　トークン12の検証値保持部
22　　トークン12の検証値出力部
23　　トークン12のトークン秘密鍵保持部
24　　トークン12の電子署名部
25　　回収装置13の履歴受信部
26　　回収装置13の履歴保持部
27　　回収装置13の履歴検証部
28　　回収装置13のトークン公開鍵保持部
29　　回収装置13の署名検証部

【図1】

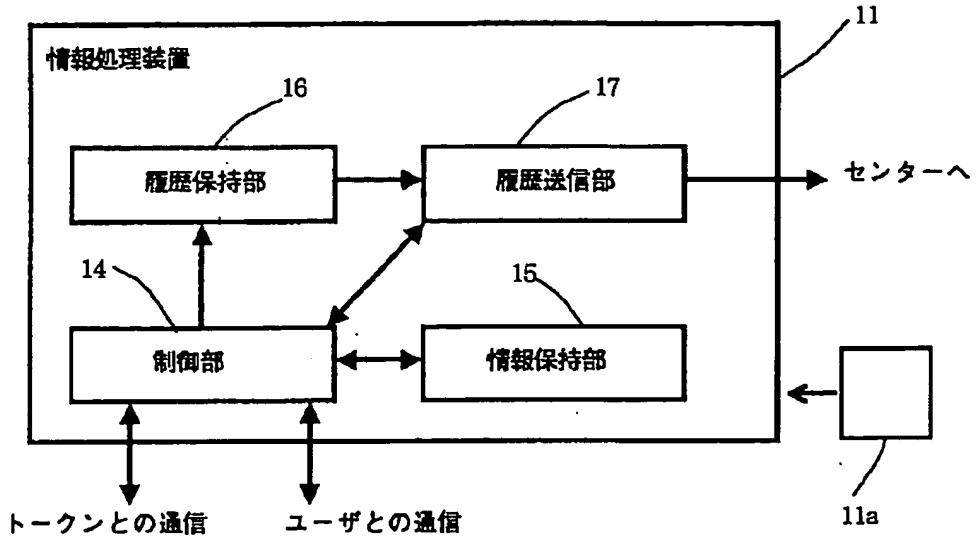


【図4】

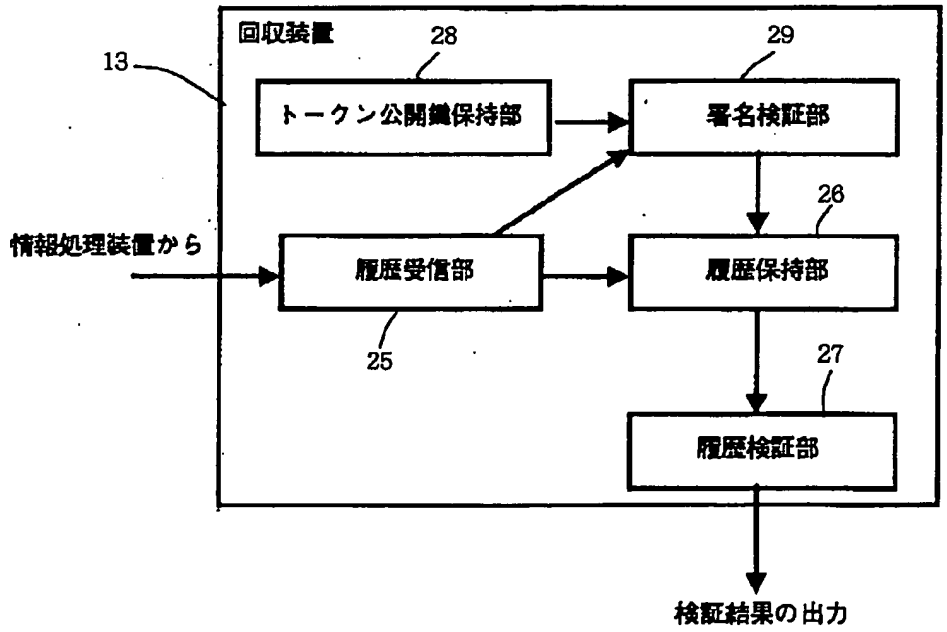
検証値
A092EF7B708B810098AFF89C046F8926

検証値保持部の内容

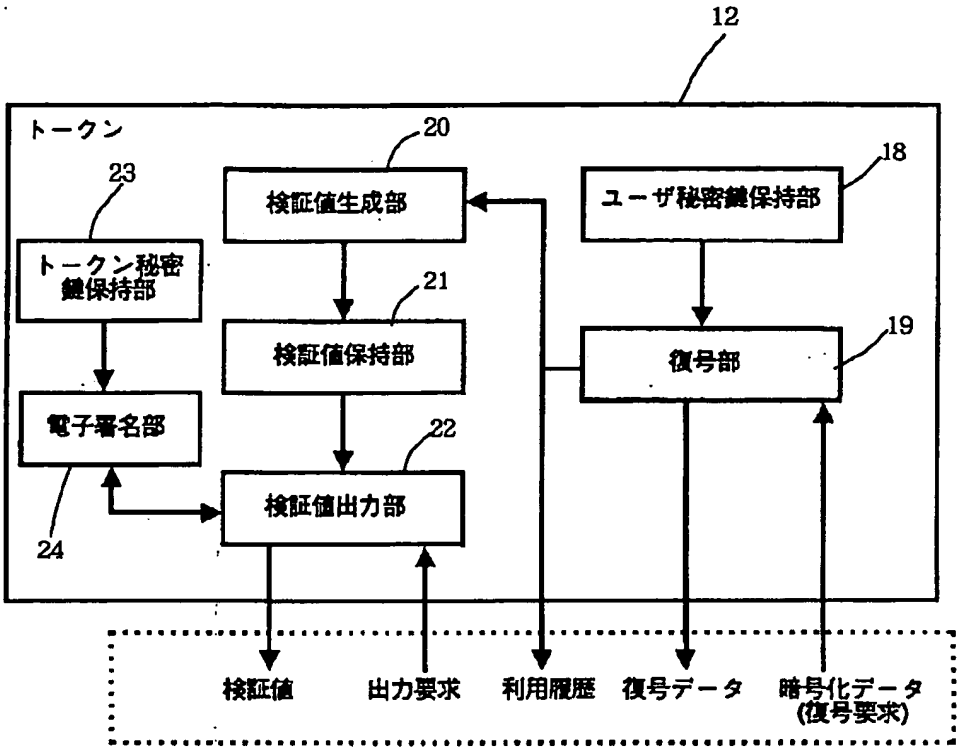
【図2】


情報処理装置
11
16
17
履歴保持部
履歴送信部
センターへ
14
15
制御部
情報保持部
11a
トークンとの通信
ユーザとの通信

【図5】


回収装置
13
28
29
トークン公開鍵保持部
署名検証部
26
情報処理装置から
履歴受信部
履歴保持部
25
27
履歴検証部
検証結果の出力

【図3】



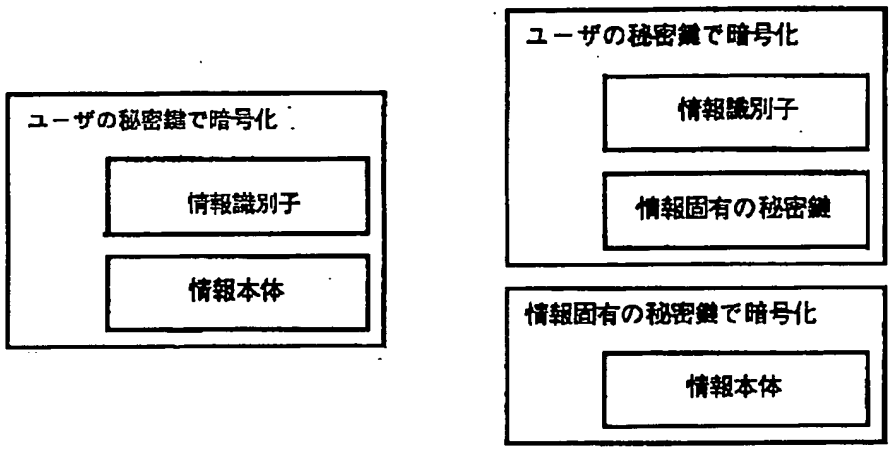
【図7】

(a) 情報処理装置の履歴保持部に記録される利用履歴

(b) 情報処理装置からセンターに送られる利用履歴

利用履歴の構成

【図6】

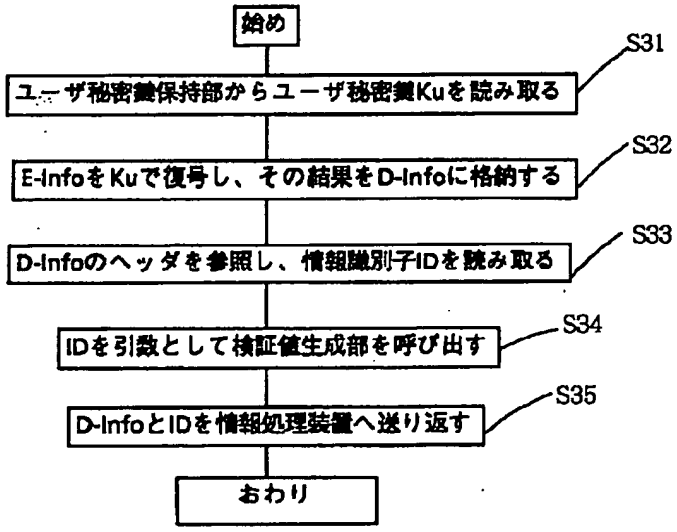


(a)情報そのものを暗号化する場合　　(b)情報そのものを暗号化する場合

暗号化された情報の構成

【図10】

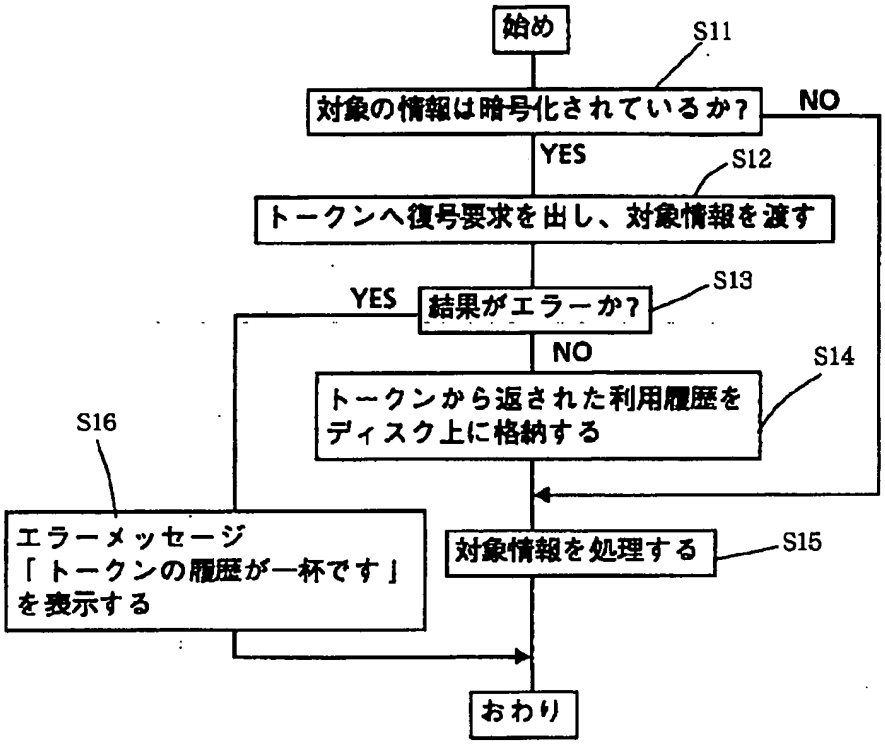
情報処理装置から暗号化された情報E-Infoの復号要求が来た時の処理



トークンの復号部の処理

【図8】

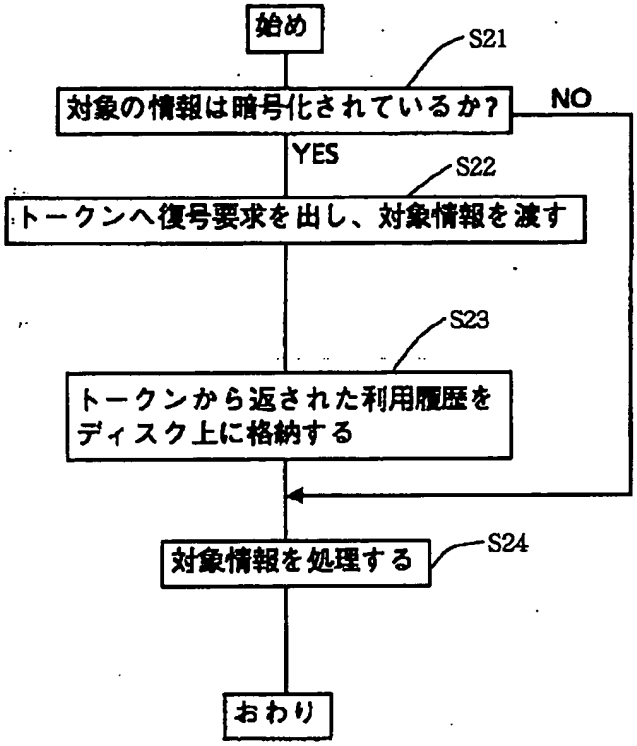
利用者から情報の利用要求が有った時の処理



情報処理装置の制御部の処理

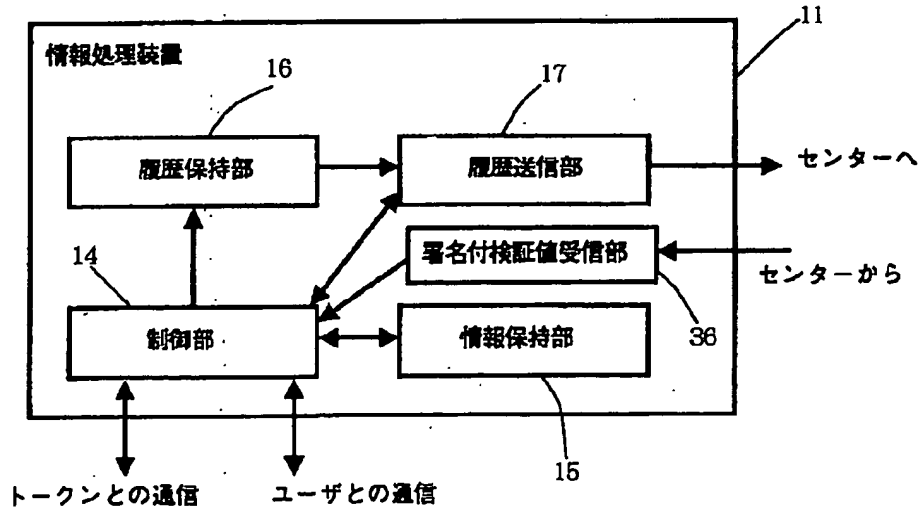
【図9】

利用者から利用履歴回収の命令が有った時の処理



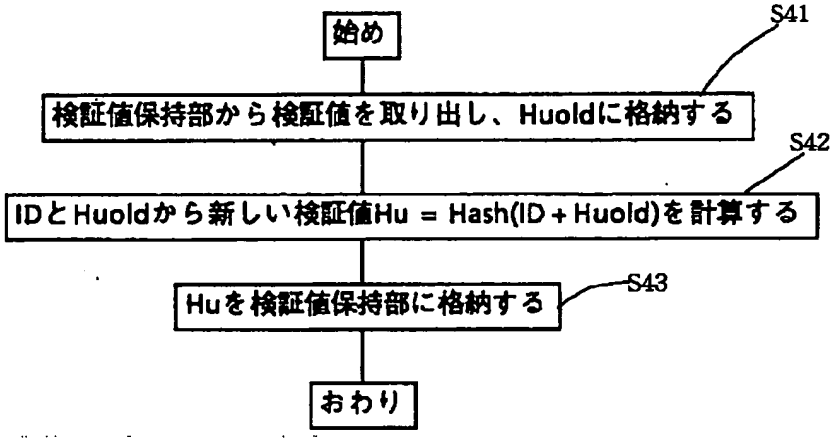
情報処理装置の制御部の処理

【図17】



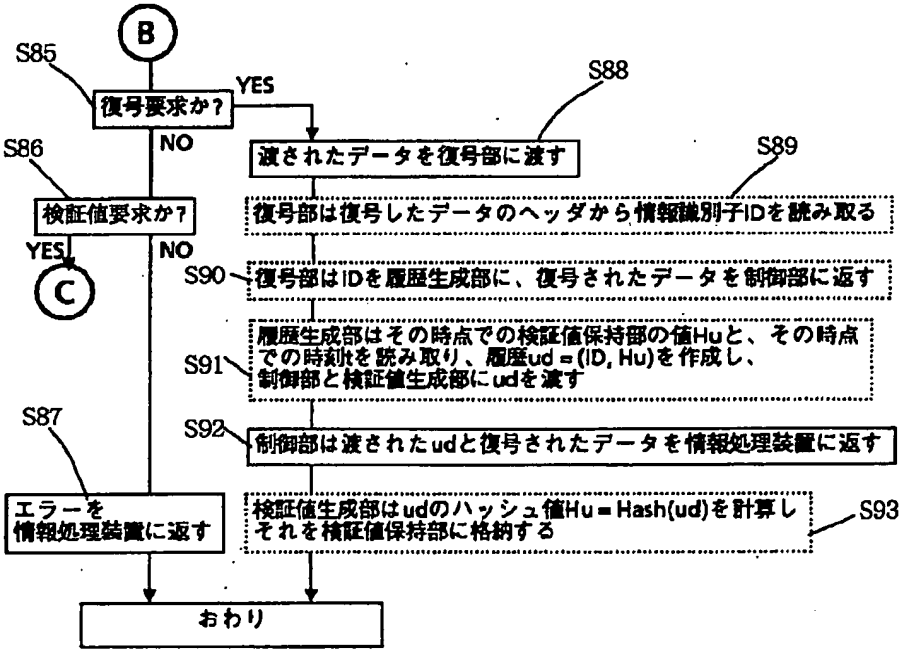
【図11】

復号部から情報識別子IDが渡されて呼び出された時の処理



トークンの検証値生成部の処理

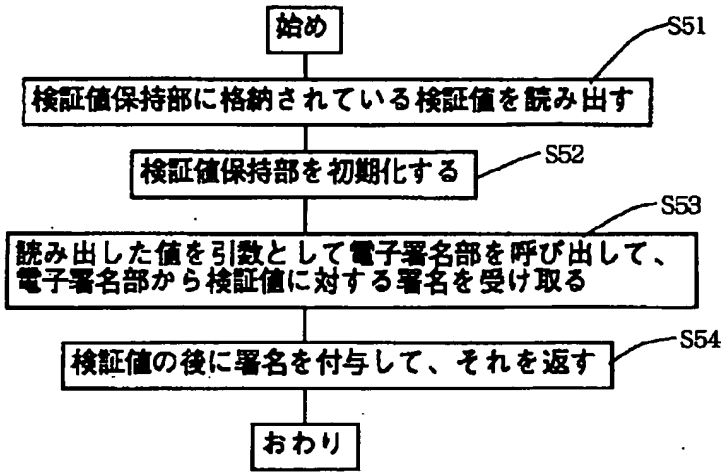
【図16】



第2の実施例のトークンの制御部の処理

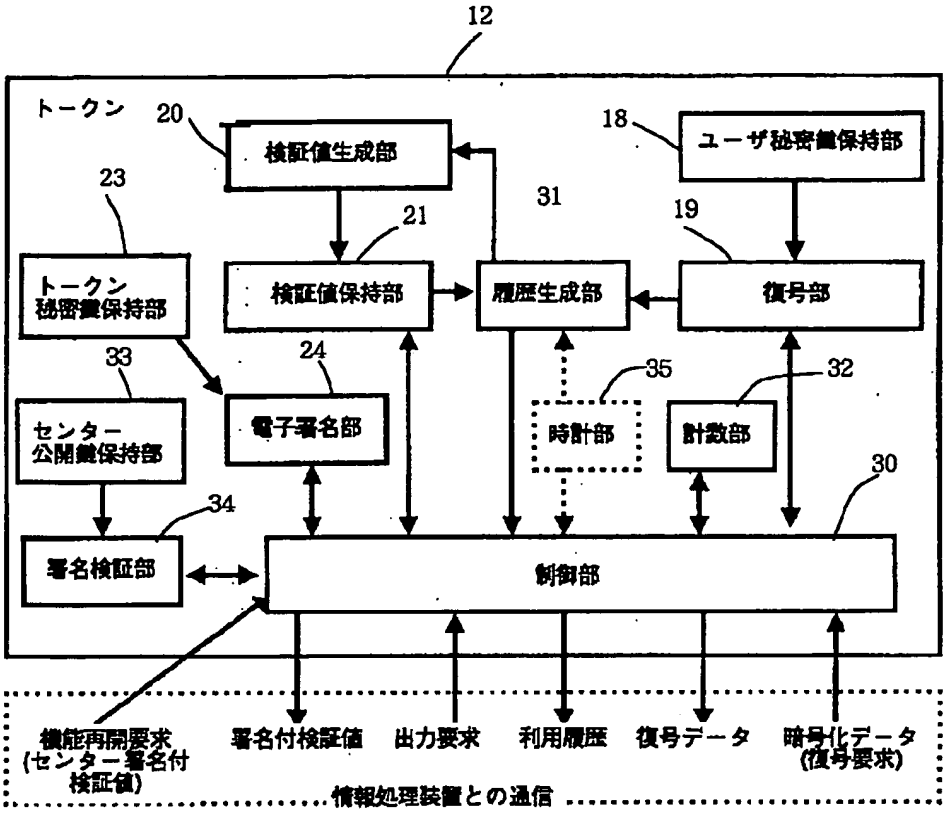
【図12】

情報処理装置から検証値出力の要求が有った時の処理

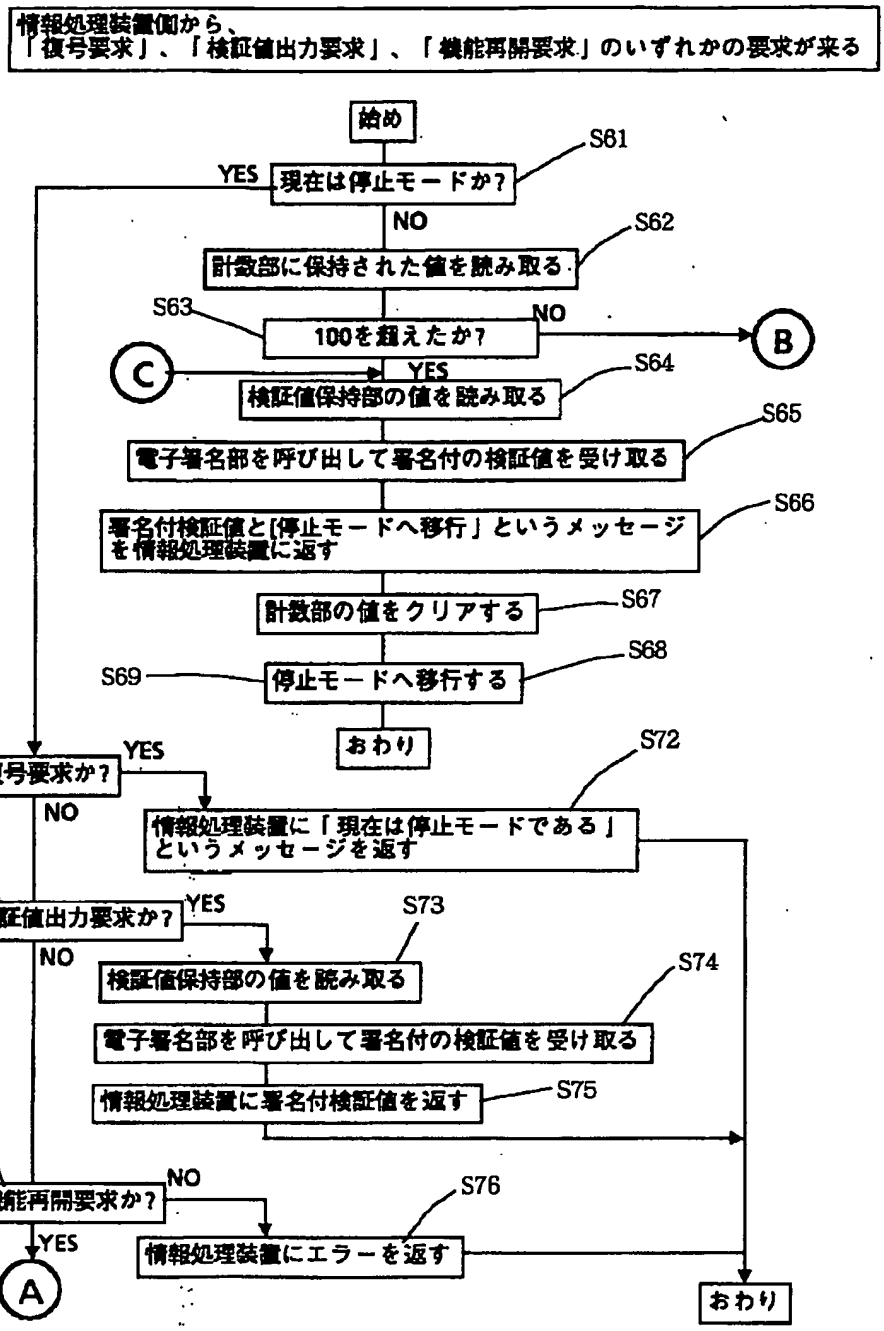


トークンの検証値出力部の処理

【図13】

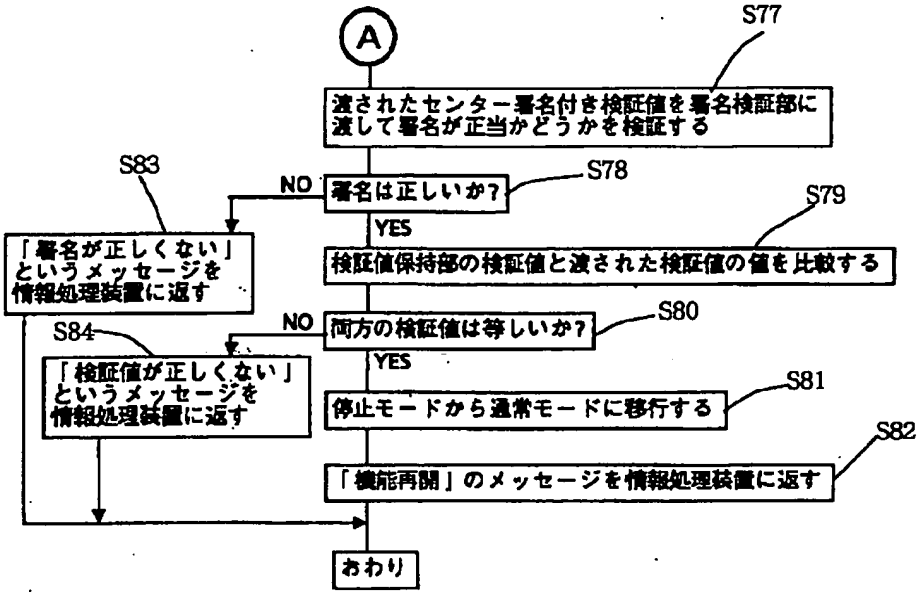

12
トークン
20
検証値生成部
18
ユーザ秘密鍵保持部
23
31
21
19
トークン
秘密鍵保持部
検証値保持部
履歴生成部
復号部
33
24
35
32
センター
公開鍵保持部
電子署名部
時計部
計数部
30
34
署名検証部
制御部
機能再開要求
(センター署名付
検証値)
署名付検証値
出力要求
利用履歴
復号データ
暗号化データ
(復号要求)
情報処理装置との通信

【図14】



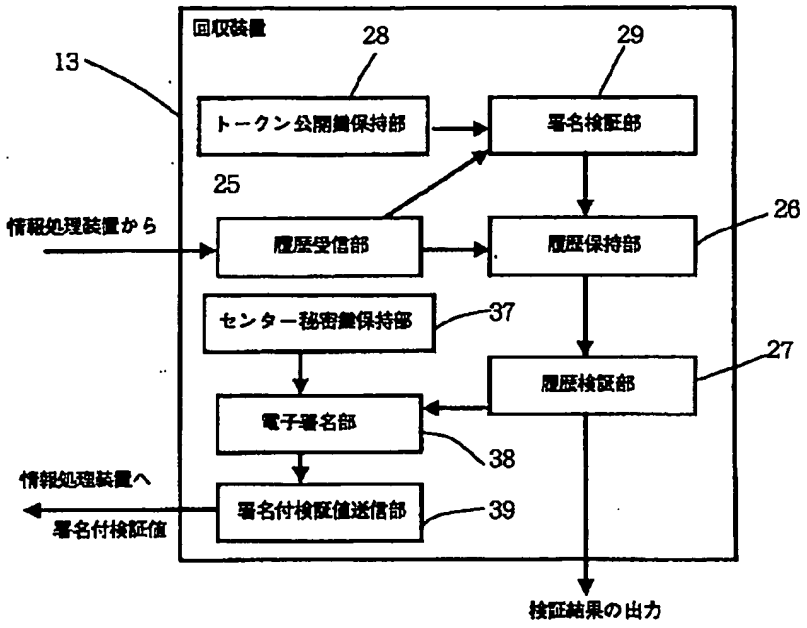
第2の実施例のトークンの制御部の処理

【図15】

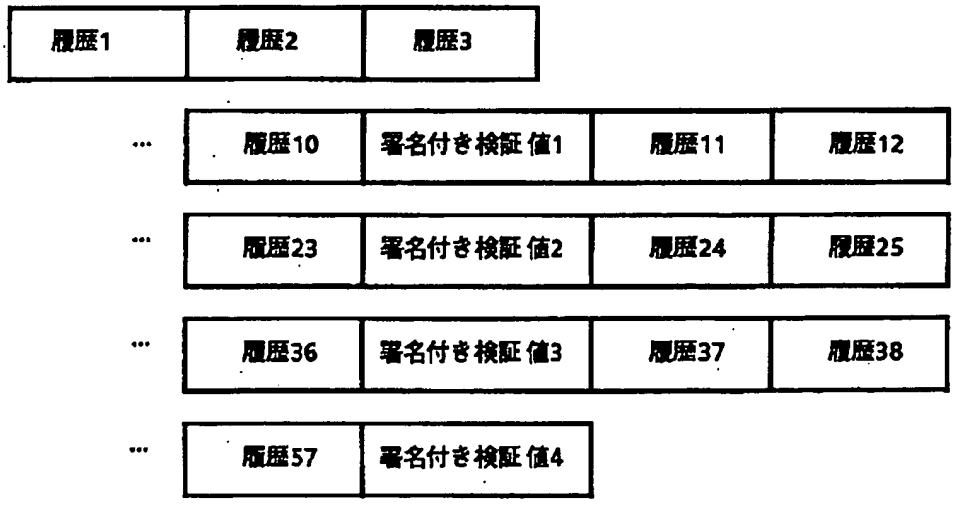


第2の実施例のトークンの制御部の処理

【図18】



【図20】

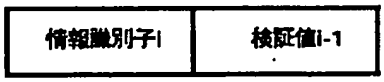


第２の実施例における利用履歴の他の構成例

【図19】

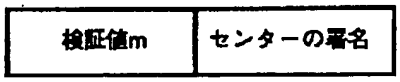
(a) 情報処理装置の履歴保持部に記録される利用履歴

(b) 情報処理装置からセンターに送られる利用履歴



(c) i番目の利用履歴の中身

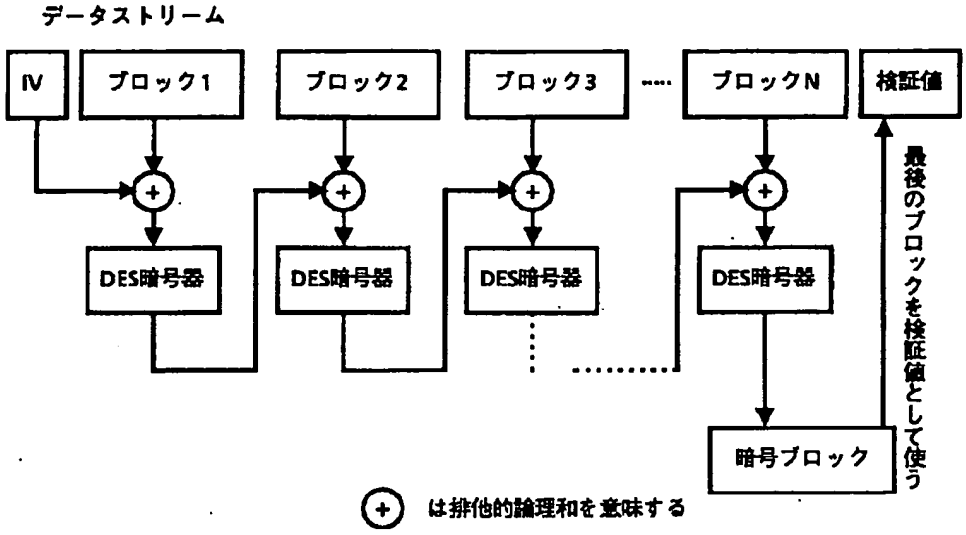
(d) 署名付検証値の中身



(e) センターから利用者に送られるメッセージ

第2の実施例における利用履歴および検証値の構成

【図21】



DES-MACの構成